PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/28, 9/00 | A1

(11) International Publication Number: **WO 00/07327**

(43) International Publication Date: 10 February 2000 (10.02.00)

(21) International Application Number: PCT/US99/17095

(22) International Filing Date: 28 July 1999 (28.07.99)

(30) Priority Data:
1998/30462 29 July 1998 (29.07.98) KR

(71)(72) Applicants and Inventors: CHOI, Jong, Uk [KR/KR]; Sung-won Apt. 2-dong #1301, Uoo eul dong, Kang-buk-ku, Seoul (KR). LEE, Won, Ha [KR/KR]; Yeunsoo-Joogoung Apt. 102-dong #1508, Yeunsoo-ku, Inchun (KR). LEE, Sang, Ki [US/US]; 540 Spring Hill Drive, Roselle, IL 60172 (US).

(74) Agents: NATH, Gary, M. et al.; Nath & Associates, 6th floor, 1030 15th Street N.W., Washington, DC 20005 (US).

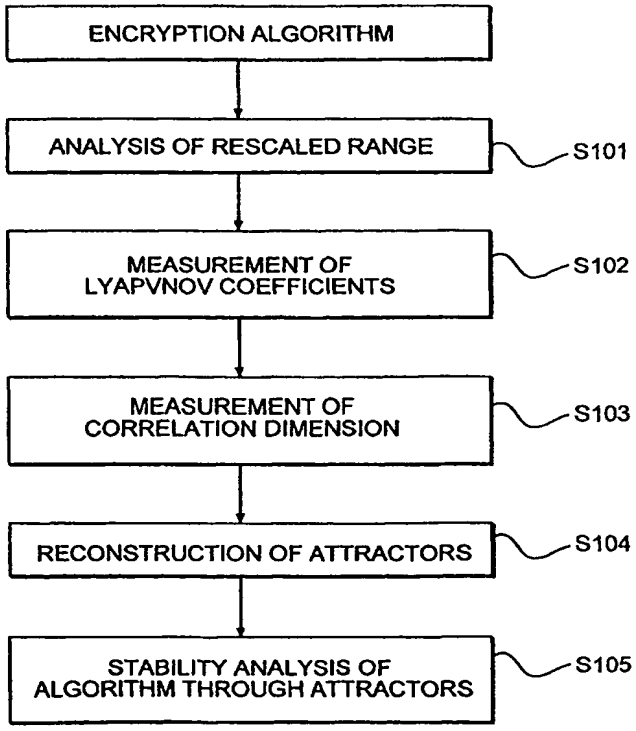
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: METHOD OF EVALUATING ENCRYPTION ALGORITHMS USING CHAOS ANALYSIS

(57) Abstract

A method of evaluating an encryption algorithm using fractal structure analysis techniques to analyze linearity or nonlinearity of the algorithm. It includes the steps of reconstructing a new phase space by mapping the output values of an encrypted message with sequentially generated key values into a time series data set, measuring the Lypunov coefficients of the time series associated with the phase space (S102), measuring the correlation dimension based on the phase space (S103), and determining the stability of the algorithm after generating attractors based on the correlation dimension (S104). The method provides improved reliability in developing encryption algorithms since it can provide a measure of the safeness of a particular encryption algorithm against possible tampering by analysing whether the algorithm is safe in the case where a new key replaces the old key, when a public or secret key becomes exposed to others.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Method of Evaluating Encryption Algorithms Using Chaos Analysis

Field of Invention

The present invention relates to a method of analyzing encryption algorithms. More specifically, the present invention relates to a method of analyzing an encryption algorithm using chaos analysis, which can analyzing non-linearity of the algorithm using the Fractal structure analysis technique in the case where a public key or a secret key become exposed to others.

Background of the Invention

With rapid advances in scientific technology and information environments, major business tasks are being performed by computers networked via a ultra-high-speed information communication network. It has become necessary to protect against theft or illegal disclosure of important information that may be scattered over various areas in a network, or information being transmitted or received through a network.

Information protection methods may be classified into a primary method of restricting physical access to the information to be protected and a secondary method of encrypting the information to be protected in case when the

first method fails.

Encryption converts a plain text to a cipher text whose meaning cannot be discerned. Decryption changes the cipher text

received to a plain text using various keys used to encrypt the text. Reliable encryption of a plain text to a cipher text requires the secrecy to allow only the authorized personnel to access the information in the computer system, the integrity to allow only the authorized personal to correct the information, and the availability to allow only the authorized personnel to use the information.

Encryption techniques may be classified into a conventional key system and a public key system, depending on the existence of a public key. In the conventional key system, both encryption and decryption use the same key. A representative example is the Data Encryption Standard (DES) announced by the U.S. Department of Commerce in 1977. In the public key system, different keys are used for encryption and decryption. Although its processing speed is slow, the public key system has an advantage of dispensing with the transmission of keys. Examples are the RAS encryption method, the Merkle-Hellmam encryption method, and the limited-body-phase encryption method, etc. However, such existing encryption systems suffer the problem of lacking data security because the safeness of encryption algorithms cannot be tested due to mathematical difficulties.

Objects of the Invention

Accordingly, it is an object of the present invention to provide reliability in developing an encryption algorithm for encrypting data being transmitted and received, by analyzing linearity or nonlinearity of the encryption algorithm, using the Fractal structure analysis, which tests whether others can predict a new key replacing the old key when a public or a secret key becomes exposed to others.

Summary of the Invention

The above and other objects are satisfied, at least in part, by an embodiment of the present invention, which provides a method including the steps of:

reconstructing a new phase space by mapping the output values of an encrypted message with sequentially generated key values into a time series data set;

measuring the Lyapunov coefficients of the data set generated with sequential modification of key values in the new phase;

measuring the correlation dimension based on the phase space; and

analyzing the stability of the algorithm by generating attractors based on the correlation dimension.

Brief Description of the Drawing

Figure 1 is a diagram of an apparatus which evaluates an encryption algorithm using chaos analysis.

Figure 2 is a flow chart showing a preferred embodiment for analyzing an encryption algorithm using chaos chart.

Detailed Description of the Drawing

References will now be made in detail to a preferred embodiment of the present invention, illustrated in the drawings.

Figure 1 illustrates a computer 100 having an encryption key generator 110 connected to an evaluator 120. Encryption key generator 110 generates encryption keys using encryption algorithms to encrypt text. Evaluator 120 determines the stability of encryption algorithms. A display device 130 being connected to computer 100 displays outputs from the computer.

When a public or secret key generated by encryption key generator 110 becomes exposed to unauthorized users, a new public or secret key must be generated. Encryption key generator
110 generates a new key to replace the old key using the encryption algorithm. In order to determine the integrity of the new key, evaluator 120 analyzes a rescaled range (R/S) of

the keys to determine the possibility of predicting the new key. Evaluator 120 generates an output displayed on display 130 which displays the stability of the encryption algorithm and will show the possibility of determining whether the new key can be predicted by others.

If an encryption algorithm does not possess the random walk property, ie, the algorithm possess the linear property, the keys generated by the algorithm may be predicted. Thus, the random walk property may be used to gauge the possibility of cracking.

Two methods are suggested for identifying the random walk property: a method based on the classical statistics and a method based on the chaos analysis which can prove nonlinearity of the system. The present invention uses chaos analysis to verify an encryption algorithm. If a system has the chaotic property , it is possible to explain and predict the system's nonlinearity because the system is deterministic.

But, a reliable encryption algorithm requires, in addition to the non-linearity element, that others may not be able to predict a new key replacing the old key when the old key was exposed to others. To determine the possibility of predicting the replacement key by others when a secret or a public key becomes exposed to others, a text encrypted using the algorithm is mapped into a continuous-time series pattern, and its property is analyzed using chaos analysis.

As shown in Fig. 1, when a public or secret key or a particular encryption algorithm used to encrypt a text becomes exposed to others and the old key is replaced by a new key, the rescaled range (R/S) of the keys for maintaining the security of a randomly selected encryption algorithm is analyzed to determine the possibility of prediction of the key by others.

The rescaled range (R/S) of the corresponding key is defined as follow:

[Equation 1]

$(R/S)_n = C \cdot n^H$ (where H is the Hurst exponent)

The average value of the rescaled range from the above equation becomes "0" meaning a local variation. Taking logarithms of both sides of the above equation yields the following:

[Equation 2]

$\log (R/S)_n = H \log(n) + \log (C)$

Since R/S in the above equation increases as fast as the increment of a square root of R/S, it is obtained through the following steps.

First, in the case of a time series of length M, it is transformed into a log ratio having the length $N = M - 1$ as follows:

[Equation 3]

$N_i = \log (M_{(i+1)}/M_i)$, where $i = 1,2,\ldots, (M - 1)$

From the above equation, a subperiod of "A", having length n and satisfying the relation $A \cdot n = N$ is obtained. Then, the label I_a (a = 1,2,...., A) is attached to each subperiod. After the value of $N_{k,a}$ (k = 1,2,...., n) are defined on each elements of label I_a, the following equation is used to calculate an average value over the length n and the label I_a:

[Equation 4]

$$e_a = (\frac{1}{n})\sum_{k=1}^{n} N_{k,a}$$

where e_a is the average value of N_i that has the length n and includes I_a.

In addition, the time series ($X_{k,a}$) representing the accumulated departures from the average values over each label I_a, is defined as follows:

[Equation 5]

$$X_{k,a} = \sum_{i=1}^{k}(N_{i,a} - e_a), \text{ where } k = 1, 2, \cdots\cdots, n$$

Therefore, from equation 4, the rescaled range R_{Ia} of the other key can be obtained from the difference between the maximum and minimum value of $X_{k,a}$ within the subperiod I_a as follows:

[Equation 6]

$R_{Ia} = Max\ (X_{k,a}) - Min\ (X_{k,a})$, where k = 1,2,....,n.

Also, the standard deviation S_{Ia} on each side label I_a is defined as follows:

[Equation 7]

$$S_{ia} = \sqrt{(\frac{1}{n}) \bullet \sum_{k=1}^{n} (N_{k,a} - e_a^2)}$$

Since the rescaled range defined in equation 6 is normalized by the ratio of standard deviation S_{Ia} as defined in equation 7, the rescaled range (R/S) is the same as R_{Ia} / S_{Ia} on each label I_a.

Since the sequential value "A" of length n can be obtained by equation 3 above, it follows that

[Equation 8]

$$(R/S)_n = (\frac{1}{A}) \bullet \sum_{a=1}^{A} (\frac{R_{Ia}}{S_{Ia}}) \text{ , where } (M - 1)/n \text{ is an integer.}$$

Here, since $(M - 1)/n$ is an integer and the length n increases to a next value, n can be used at the starting and ending points of the time series by repeating the above process up to $n - (M - 1)/2$. Accordingly, least squared regression is performed on a graph plotted using $\log(n)$ as an independent variable and $\log(R/S_a)$ as a dependent variable, and the Hurst exponent "H" can be obtained from the slope of the graph.

After obtaining the Hurst exponent "H" in the rescaled range

R/S through the same process as stated above, measurement of

Lyapunov exponents is conducted at step 102. The Lyapunov exponent (L) in i dimension ($p_i(t)$) is measured as follows:

[Equation 9]

$$L_i = \lim_{t \to \infty} \left(\frac{1}{t}\right) \log_2 \left(\frac{p_i(t)}{p_i(0)}\right)$$

Since one must have input data, the embedding dimension, the time lag, the evolution time, the max/min distance, and the mean orbital period to measure the Lyapunov exponents, the embedding dimension is obtained from the correlation integral Cm; the time lag from the relation $m*t(delay) = Q(period)$; the mean orbital period from the analysis of the reconstruction range; the max/min distance from the embedding dimension.

Once the input data, the embedding dimension, the time lag, the evolution time, the max/min distance, and the mean orbital period are determined, the distance between two points $(DI) - L_1(X_0)$, separated at least by the mean orbital period, is measured, and the interval for measuring the Lyapunov exponent, $(DF) - L_1(X_0)$, is determined. Then the Lyapunov exponent is initialized as follows:

[Equation 10]

$$SUM = \frac{1}{t}\sum_{j=1}^{m} \log_2\left(\frac{L(x_{j+1})}{L(x_j)}\right) + SUM$$

$$_2Lyap = [SUM / Iteration]$$

In the above, if the measurement distance of Lyapunov exponent *DF* > *Dist_Max* and *DF* < *Dist_min*, a new point, "*DN*' is selected. In this case, the time interval of the newly selected point must be at least one period. The new point must be between the min and the max distances, and the angle between *DN* and *DF* must be minimum in the phase space. If a new point is selected, *DI* is set to *DN*, and the steps of initializing the Lyapunov coefficient are repeated.

Once the measurement of Lyapunov exponents is completed using the steps above, measurement of a correlation dimension is performed at step 103. Although the correlation dimensions are observed as one of the coefficients of the time series, it has a limitation of having value between 1 and 2. However, in the case of reconstructing a time series in a phase space, since it is possible to observe all independent coefficients, the correlation dimension (m), starting from m=2, is measured, by increasing the diameter of Fractal structure using the following equation:

[Equation 11]

$$C_m(R) = (\frac{1}{N^2}) * \sum_{i,j=1}^{N} Z(R - |x_i - x_j|)$$

where $Z(x) = 1$ if $R - |x_i - x_j| > 0$; otherwise N is the observation constant, R is the distance, and C_m is the correlation dimension integral function m.

$Z(x)$ is called a Heaviside function. A correlation

dimension means a probability that there will be two points within the Fractal diameter between t and $t-1$. The correlation dimension is derived by measuring the slope of a graph of log $(C_m[R])$ versus log($[R]$) based on the above result.

Once the correlation dimension is derived, attractors are reconstructed at step 104. For example, a random time series pattern having n numbers of data with their sampling interval of

δt is expressed as $X(t)$, $X(t + \delta t)$, $X(t + 2 \cdot \delta t)$, $X(t + 3 \cdot \delta t)$,...., $X(t + (n-1) \cdot \delta t)$. After setting the time lag (T) to twice the sampling time δt(T = 2 δt), a three-dimensional vector column is obtained, expressed as $X(t)$, $X(t + 2 \cdot \delta t)$, $X(t + 4 \cdot \delta t)$, $X(t + 1 \cdot \delta t)$, $X(t + 3 \cdot \delta t)$,..., $X(t + (n-5) \cdot \delta t)$, $X(t + (n-3) \cdot \delta t)$, $X(t + (n-1) \cdot \delta t)$.

By plotting these points in the three-dimensional space, a three-dimensional attractor may be obtained showing the dynamic property of the system. If the value of n equals or is larger than the original dimension and is properly selected, the vector column will show the same dynamic property as the original movement.

The strange attractor reconstructed by the same method described above, in general, has a transformed shape, not precisely the same shape as the original attractor. However, since the Lyapunov exponent and the Fractal dimension are not

altered by such a transformation, these values can be calculated from the reconstructed attractor.

As explained above, the present invention provides reliability and safeness in developing an encryption algorithm by providing a method for determining the safeness of the algorithm where a new key replaces the old when a public key or secret key becomes exposed to others.

What is claimed is:

1. A method for evaluating an encryption algorithm using chaos analysis, comprising the steps of:

obtaining Hurst exponent in the analysis of a rescaled range with sequential generation of key values of encryption;

measuring Lyapunov coefficients;

measuring the correlation dimension based on a time series reconstructed in phase space;and

determining stability of the algorithm after constructing attractors based on the correlation dimension.

2. The method of claim 1, wherein the step of analyzing a rescaled range further comprises the steps of:

transforming the rescaled range into a log ratio value of length $N = M - 1$ where M is the length of the time series;

calculating a mean value n and I_a where n is the length of a subperiod and I_a is a label that attaches to the subperiod;

calculating accumulated departure of the time series and its range;

calculating standard deviation for each said I_a and then calculating starting and ending points of the time series; and

obtaining the Hurst exponent using least square regression.

3. The method of claim 1, wherein the step of measuring the Lyapunov coefficients further comprises of steps of:

measuring at least one orbital period by measuring the distance between selected two separate points, $(DI) - L1(x_a)$;

determining measurement distance of the Lyapunov exponent, $(DF) - L1(x_1)$, and then initializing the Lyapunov exponent;

selecting a new point "DN" if said measurement distance of the Lyapunov exponent $DF > Dist_Max$ and $DF < Dist_min$; and

setting DI to DN, and repeating the above steps, including initializing of the Lyapunov exponent, if the new point is selected.

4. The method of claim 1, wherein the step of measuring a correlation dimension further comprises the steps of:

increasing embedding dimension (m) from $m = 2$;

increasing a diameter of Fractal structure; and

drawing a graph to measure the correlation dimension.

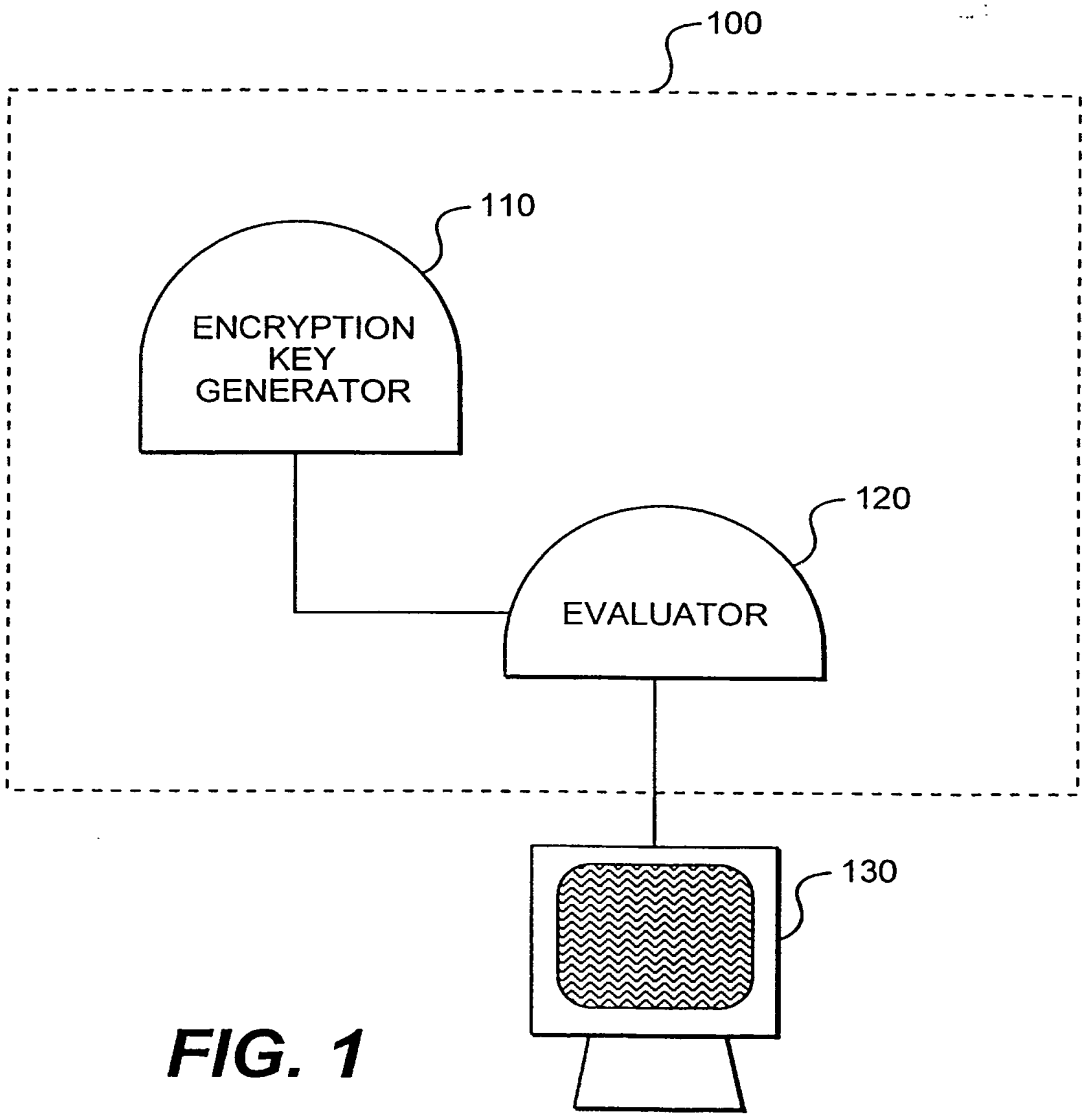


FIG. 1

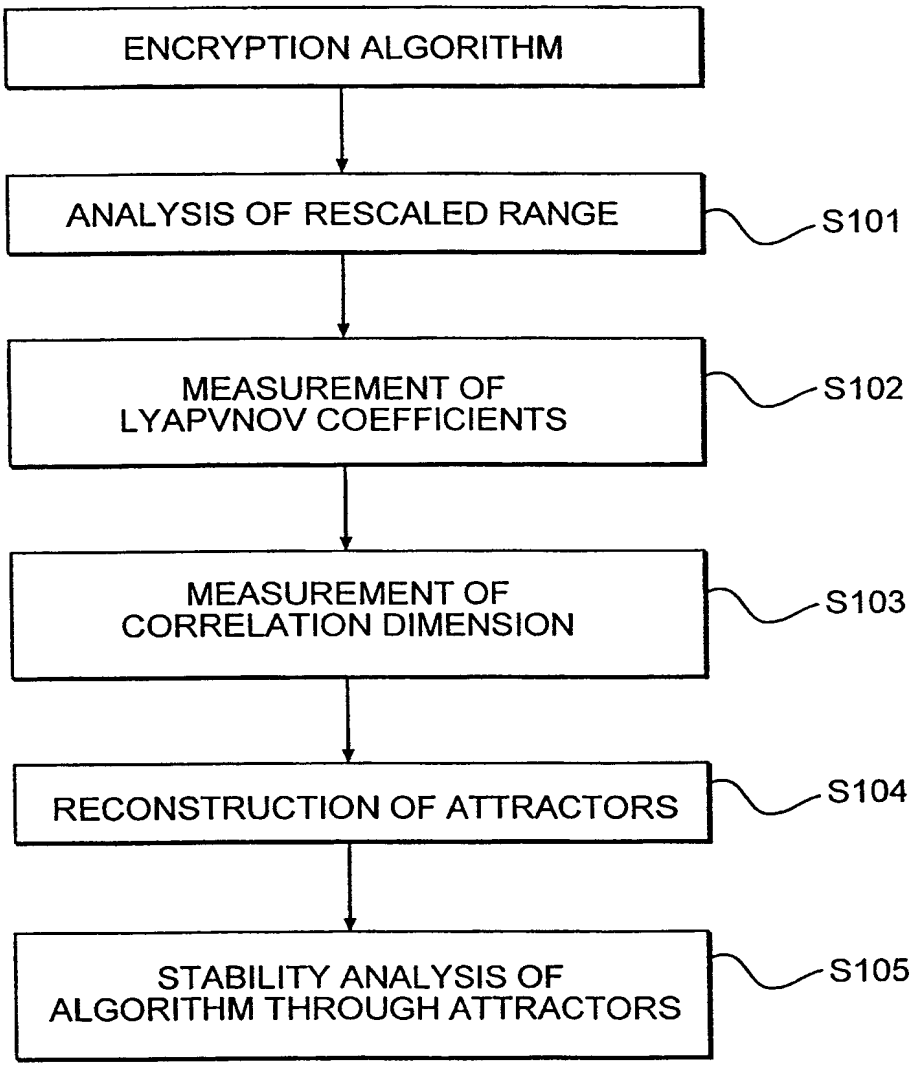

ENCRYPTION ALGORITHM
ANALYSIS OF RESCALED RANGE
S101
MEASUREMENT OF LYAPVNOV COEFFICIENTS
S102
MEASUREMENT OF CORRELATION DIMENSION
S103
RECONSTRUCTION OF ATTRACTORS
S104
STABILITY ANALYSIS OF ALGORITHM THROUGH ATTRACTORS
S105

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No. PCT/US99/17095

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/28, 9/00

US CL : 380/28, 46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, Dialog, and Internet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	F. DACHSELT et al, Chaotic Coding and Cryptoanalysis, 1997	1-4
Y	M. J. OGORZATEK ET AL, Some Tools for Attacking Secure Communication Systems Employing Chaotic Carriers, 1998	1-4
Y	L. KOCAREV et al, From Chaotic Maps to Encryption Schemes	1

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search: 30 AUGUST 1999

Date of mailing of the international search report: 25 OCT 1999

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer: Gail Hayes

Telephone No. (703) 308-4562

Form PCT/ISA/210 (second sheet)(July 1992) *

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/17095

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	YANG, TAO et al. Cryptography Based on Chaotic Systems, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications 44(5), May 1997, 469-472	1-4
Y	US 5,048,086 A [BIANCO et. al.] 10 september 1991, col. 2-6	1
Y	US 5,696,828 A [KOOPMAN, JR.] 09 December 1997, col 4-9	1
Y	US 5,751,811 A [MAGNOTTI et. al.] 12 May 1998, col. 5-10	1-4
Y	HAYES et. al. Experimental Control of Chaos for Communications, P hysical Review Letters, 26 September 1994	1
Y	EDWARD OTT et. al. Controlling Chaos, Physical Review Letters, 64(11) pages 1196-1199, 12 March 1990	1
Y	DING et. al. Enhancing Synchronism of Chaotic Systems, 49(2) Physical Review E, February 1994, pga R945-948	1-4
Y	US 5,680,462 A [MILLER et. al.] 21 October 1997, col 4-20	1-4